UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,495	10/28/2003	Nadarajah Asokan	915-008.013	5756

4955 7590 11/09/2009

WARE FRESSOLA VAN DER SLUYS & ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
11/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/696,495	ASOKAN ET AL.	
	Examiner	Art Unit	
	CANH LE	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-9,11-18,20-25 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-9,11-18,20-25 and 27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the communication filed on 07/31/2009.

Claims 2, 10, 19, and 26 have been cancelled.

Claims 1, 7-9, 15, 17-18, 25, and 27 have been amended.

Claims 1, 3-9, 11-18, 20-25, and 27 have been examined and are pending.

Response to Arguments

Applicant's arguments, see page 10, filed 07/31/2009, with respect to the 35 U.S.C. 112, 2nd rejection of claims 6 and 15 have been fully considered. The 35 U.S.C. 112, 2nd rejection of claims 6 and 15 has been withdrawn due to amendment.

Applicant's arguments, see page 9, filed 07/31/2009, with respect to the 35 U.S.C. 101, the rejection of claim 27 have been fully considered but they are not persuasive. The 35 U.S.C. 101, the rejection of claim 27 is maintained for the following reasons:

The Examiner reviews the specification shows in figure 1 a system which includes the elements for performing the operations means plus function elements in claim 27. A box include a secure processing point 150 with processing means 155 for performing recited functions as specified in the application as filed, including page 9, line 24 through page 15, line 24, including the various action recited and illustrated in step 1-8. However, there is *no sufficient support for* **"means for"** languages and there is no structure disclosed in the specification.

Applicant's arguments, see page 10, filed 07/31/2009, with respect to the 35 U.S.C. 112, 2nd rejection of claim 27 have been fully considered but they are not persuasive. The 35 U.S.C. 112, 2nd rejection of claim 27 is maintained for the following reasons:

The Examiner reviews a box include a secure processing point 150 with processing means 155 for performing recited functions as specified in the application as filed, including page 9, line 24 through page 15, line 24, including the various action recited and illustrated in step 1-8; However, there is *no sufficient support for* "means for" languages and there is no structure disclosed in the specification.

The Applicant's arguments with respect to claims 1, 3-9, 11-18, 20-25, and 27 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

Claims 1, 15, 17, and 27 are objected to because of the following informalities: Appropriate correction is required.

(Claim 1, line 5): "a personal device" should be replaced by "the personal device" to avoid antecedent basis.

(Claim 1, line 21): "the device" should be replaced by "the personal device" to avoid antecedent basis.

(Claim 1, line 14): "the associated unique chip identifier" should be replaced by "an associated unique chip identifier" to avoid antecedent basis.

(Claim 15, line 6): "the device" should be replaced by "the personal device" to avoid antecedent basis.

Claim 17 recites "a method comprising: receiving from the public database a backup data package which has been assembled and stored in accordance with claim 1 and corresponding to the transmitted chip identifier" is improper *(See MPEP 608.01 (n), "Infringement Test" for dependent claims. The test for a proper dependent claim is whether the dependent claim includes every limitation of the parent claim. The test is not whether the claims differ in scope. A proper dependent claim shall not conceivably be infringed by anything which would not also infringe the basic claim).*

(Claim 27, line 5): "a personal device" should be replaced by "the personal device" to avoid antecedent basis.

(Claim 27, line 16): "the associated unique chip identifier" should be replaced by "an associated unique chip identifier" to avoid antecedent basis.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 3-9, 11-16, 17, 18, 20-25, and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the personal device" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 1 recites the limitation "signing ***the result*** of said "***associating***" in line 18. It is unclear "***said associating***" as to whether refers to "***associating*** *the unique chip identifier with the received backup data package*" in line 13 ***or*** "***associating*** *a unique device identity with the unique chip identifier*" in line 17 (emphasis added).

Claim 1 recites the limitation "***the result*** of said "***associating***" in line 18. It is indefinite to what a "result" of the "associating" is.

Claim 9 recites the limitation "signing ***the result*** of said "***associating***" in line 21. It is unclear "***said associating***" as to whether refers to "***associating*** *the unique chip identifier"* in line 17 ***or*** "***associating*** *a unique device identity with the unique chip identifier*" in line 20 (emphasis added).

Claim 9 recites the limitation "***the result*** of said "***associating***" in line 21. It is indefinite to what a "result" of the "associating" is

Claim 25 recites the limitation "signing ***the result*** of said "***associating***" in line 14. It is unclear "***said associating***" as to whether refers to "***associating*** *the unique chip identifier"* in lines 11-12 ***or*** "***associating*** *a unique device identity with the unique chip identifier*" in line 13 (emphasis added). Claim 25 recites the limitation "***the result*** of said "***associating***" in line 14. It is indefinite to what a "result" of the "associating" is.

Claim 27 recites the limitation "signing ***the result*** of said "***associating***" in line 20. It is unclear "***said associating***" as to whether refers to "***associating*** *the unique chip identifier"* in line 16 ***or*** "***associating*** *a unique device identity with the unique chip identifier*" in line 19 (emphasis added).

Claim 27 recites the limitation "***the result*** of said "***associating***" in line 20. It is indefinite to what a "result" of the "associating" is.

Claim 3 recites the limitation "the at least one cryptographic key includes ***at least one key*** to be used for a secure, key based communication channel a personal device manufacturer and the personal device". It is unclear as to whether "***at least one key"*** means *"cryptographic keys that are specific to a personal device"* or *"a unique secret chip key".*

Claim 11 recites the limitation "the at least one cryptographic key includes ***at least one key*** to be used for a secure, key based communication channel a personal device manufacturer and the personal device". It is unclear as to whether "***at least one key"*** means *"cryptographic keys that are specific to a personal device"* or "*a unique secret chip key".*

Claim 18 recites the limitation "the public database" in line 14. There is insufficient antecedent basis for this limitation in the claim.

Claim 22 recites the limitation "the unique device identity" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 24 recites the limitation "the unique device identity" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 20 recites the limitation "the at least one cryptographic key includes ***at least one key*** to be used for a secure, key based communication channel a personal device manufacturer and the personal device". It is unclear as to whether "***at least one key"*** means *"cryptographic keys that are specific to a personal device"* or *"a unique secret chip key"*.

Claim 25 recites the limitation "the device" in lines 16-17. There is insufficient antecedent basis for this limitation in the claim.

Claim 25 recites the limitation *"a **read-only storage**"* in line 4 and *"associating a unique device identity with the unique chip identifier; signing the result of the association with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a **read-only memory** of the device, thereby generating a certificate for the unique device identity; storing the certificate in the device; and storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database."* in lines 13-19. It is unclear the relationship between "***a read-only memory***" and "***a read-only storage***".

Claim 27 recites the limitation "the personal device" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 27 has been found in valid as indefinite because the claim recites ***"means for"*** languages and there is no structure disclosed in the specification. *"If there is no structure in the specification corresponding to the means-plus-function limitation in the claims, the claims will be found invalid as indefinite." Biomedino, LLC vs. Waters Technology Corp.*, 490 F.3d 946, 950 (Fed. Cir. 2007).

Regarding to claims 1, 9, 25 and 27, Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "**a certificate**" in **claims 1, 9, 25 and 27** is used by the claims to mean "*signing the result of said associating with a manufacturer private signature key* corresponding to a manufacturer public signature key stored in a read-only memory of the personal device, *thereby generating* **a certificate** for the unique device identity", while the accepted meaning is "*a certificate is sent when a message is digitally signed. The certificate proves the sender's identity and supplies the recipient with a public key with which to decrypt the sender's encrypted messages (Microsoft Computer Dictionary, Fifth Edition, page 93, 2002)*" . The term is indefinite because the specification does not clearly redefine the term.

Claims 3-8 and 17 are dependent on claim 1, and therefore inherit the 35 U.S.C 112, second paragraph issues of the independent claim.

Claims 11-16 are dependent on claim 9, and therefore inherit the 35 U.S.C 112, second paragraph issues of the independent claim.

Claims 20-24 are dependent on claim 18, and therefore inherit the 35 U.S.C 112, second paragraph issues of the independent claim.

The Examiner kindly requests the Applicant to point out with specificity (i.e. column and line) in the specification where it describes/supports the aforementioned limitation.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 27 is rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Regarding claim 27, the claims are not directed to eligible subject matter in view of ***In re Comiskey***, 499 F.3d 1365 (Fed. Cir. 2007). Although the preamble of claim 27 recites "A device", the bodies of the claims do not positively recite any elements of hardware. The claim merely recites *"means for retrieving," "means for assembling," "means for receiving," "means for associating," "means for storing," and "means for signing",* and do not positively recite any element of hardware or machine (e.g., a computer), which the aforementioned "means for" are tied to. There is no further disclosure in the specification as to how "means for" claimed are implemented. The aforementioned "means for" could be implemented using software by one of ordinary skill in the art at the time the invention was made; therefore, the nature of the subject matter claimed may reasonably be construed as a mental process since the language of claims 24 and 37 broadly encompasses non-tangible embodiments. See ***In Re Bilski***, 88 USPQ2d 1385; see also ***Diamond v. Diehr***, 450 U.S. 175, 184 (1981); ***Parker v. Flook***, 473 U.S. 584, 588 n.9 (1978); ***Gottschalk v. Benson***, 409 U.S. 63, 70 (1972); ***Cochrane v. Deener***, 94 U.S. 780, 787-88

(1976)); The mere recitation of the machine in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-4, 6, 8-9, 11-12, 14, 16-17, 25, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mauro** (US 2002/0147920) in view of **Craft** et al. (US 2002/0150243) further in view of **Chien** (US 7,551,913 B1), and further in view of **Okimoto** et al. (US 6,978,022 B2),

As per claim 1:

Mauro teaches a method comprising:

(a) retrieving in a secure processing point separated from and arranged in communication with the personal device, a unique chip identifier from a read-only storage of an integrated circuit chip included in a personal device **[Mauro: par. [0038]); A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier) via a secure operation (e.g., during the manufacturing phase) and become available for use thereafter (e.g. retrieving a unique chip identifier)]**;

(b) the secure processing point assembling a data package and loading the data package in the personal device for storage therein, the data package including at least one cryptographic key specific to the personal device **[Mauro: par. [0034], lines 1-7; A secure unit 240 to perform all secure processing and store all "sensitive" data (e.g. cryptographic key) by various cryptographic technique]**;

storing sensitive data in a tamper-resistant secret storage of chip an integrated circuit chip included in the personal device **[Mauro: par. [0037]; memory 254 is a non-volatile memory that may be used to stored sensitive data; par. [0039]; "secure processor 250 and memory 254 are implemented as two separate units enclosed within secure/or tamper resistance/evident unit"]**;

(l) storing the certificate in the device **[Mauro: par. [0010]; storing certificate in secure storage of data]**;

(m1) storing the unique device identity and the certificate **[Mauro: par. [0010]; storing certificate in secure storage of data; par. [0055]; the certificate is issued and signed by a trusted certificate authority that certifies the remote terminal's identity; par. [0063]; certificate containing identity verification information for the remote terminal].**

Mauro does not explicitly disclose,

(c) receiving at the secure processing point, in response to storing the data package, a backup data package from the personal device, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage of the integrated circuit chip included in the personal device;

(d) associating the unique chip identifier with the received backup data package; and

(e) storing the backup data package and the associated unique chip identifier in a permanent public database separated from the personal device:

(f) wherein the secure processing point further performs:

(g) associating a unique device identity with the unique chip identifier;

(h) signing the result of said associating with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the personal device, thereby generating a certificate for the unique device identity;

(m) storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database.

However, Craft discloses,

(c) receiving at the secure processing point, in response to storing the data package, a backup data package from the personal device, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage of chip **[Craft: fig: 2; par. [0021] and par. [0019]; A server system receives encrypted content data using permanent, hardware-embedded, cryptographic keys (tamper-resistant secret storage) from a client.]**

(d) associating the unique chip identifier with the received backup data package **[Craft: par. [0041], lines 7-13; "The manufacture of the client CPU chips also has knowledge of a server public key that is associated with a server private key that may or may not be known to the manufacturer"];**

(e) storing the backup data package and the associated unique chip identifier in a permanent public database separated from the personal device **[Craft: par. [0043], lines 1-6 and**

figure 2; A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database].

(f) Craft further discloses the secure processing point performs:

(g1) associating a unique device identity with the unique chip identifier **[Craft: par. [0015]; par. [0041]; a unique device identity is associated with client device ; CPU chip is equivalent to unique chip identifier];**

(h) signing the result of said associating with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity **[Craft: par. [0036]; "a data can be signed by computing a digital signature from the data and the private key of signer"; a data signed by computing a digital signature using private key, thereby generating a certificate];**

(m) storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database **[Craft: par. [0043], lines 1-6 and figure 2; A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database]**.

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the method of Mauro by including other feature such as receiving in response to storing the data package, associating the unique chip identifier with the received backup data package , and storing the backup data package and the associated unique

chip identifier of Craft because it would ensure security of the communication between client devices and servers **[Craft: paragraph [0013], lines 1-4, Craft et al.]**

Mauro and Craft are not so clear of disclosing a unique device identity and associating a unique device identity with the unique chip identifier;

However, Chien discloses methods and apparatus for anonymous user identification and content personalization in wireless communication, wherein associating a unique device identity with the unique chip identifier **[Chien: Col. 3; lines 15-20; Col. 3, lines 55-60; Col. 4, lines 1-32; fig. 1; Wireless communication device includes a device serial number 102 and a SIM_ID 107; Col. 4, lines 28-32; An International Mobile Station Equipment Identity (IMEI) can be used as a device identifier; fig. 2; Col. 4, lines 40-50; retrieving personalization parameters such as a device serial number as a SIM_ID; Col. 6, lines 54-57].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the method of Mauro and Craft by including the teaching of Chien wherein associating a unique device identity with the unique chip identifier to provide anonymous content personalization in wireless communication network **[Chien: Col. 2, lines 34-42].**

Although the combination of Mauro, Craft, and Chien teach the claimed subject matter, they are not so clear of disclosing the secure processing point being separated from the personal device. On the hand, Okimoto teaches this limitation in Column 5 **[Okimoto: Col. 5, lines 52-53].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Mauro, Craft, and Chien by including teaching of Okimoto because it would securely deliver encrypted content on demand with access control **[Col. 3, lines 67 to Col. 4, line 1, Okimoto].**

As per Claim 3:

The combination of teaching Mauro, Craft, Chien, and Okimoto teach the claimed subject matter.

Craft et al. further disclose wherein the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device **[Craft: par. [0038], figure 2; "a data processing system for secure communication of application code and content using permanent, hardware-embedded, cryptographic key"].**

As per Claim 4:

The combination of teaching Mauro, Craft, Chien, and Okimoto teach the claimed subject matter.

Craft et al. further disclose the method as claimed in claim 3, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key **[Craft: par. [0038], lines 1-5; par. [0060], lines 20-24. The symmetric key is a cryptographic key which uses trivially cryptographic key for both decryption and encryption].**

As per Claim 6:

The combination of teaching Mauro, Craft, Chien, and Okimoto teach the claimed subject matter.

Craft et al. further disclose the method as claimed in claim 3, wherein the at least one key to be used for a secure, key based communication channel includes a private/public key pair **[Craft: par. [0038], par. [0032], "Public key cryptography requires each party involved in a communication or transaction to have a pair of key, called the public key and the private key"].**

As per Claim 8:

The combination of teaching Mauro, Craft, Chien, and Okimoto teach the claimed subject matter.

Craft et al. and Chien further disclose wherein the personal device is a wireless communications terminal and the unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network **[Craft: par. [0025], lines 13-16. Personal digital assistant (PDAs, client 107) is equivalent to a wireless personal device; Chien: Col. 3; lines 15-20; Col. 3, lines 55-60; Col. 4, lines 1-32; fig. 1; Wireless communication device includes a device serial number 102 and a SIM_ID 107].**

As per claim 9:

Mauro teaches a system comprising:

(a) at least one personal device **[Mauro: fig. 1, box 110a; fig. 2]**, and

(b) a secure processing point **[Mauro: fig. 2, box 240]**, which secure processing point is separated from and arranged in communication with the personal device,

(c) wherein the at least one personal device includes an integrated circuit chip with a unique chip identifier in a read-only storage and a unique secret chip key in a tamper- resistant secret storage **[Mauro: par. [0038], lines 1-4. A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier); par. [0039], lines 9-11; "secure processor 250 and memory 254 are implemented as two separate units enclosed within a secure and/or tamper resistance/evident unit]**;

(d) wherein the secure processing point includes a processor configured for retrieving the unique chip identifier and for assembling a data package and loading the data package in the personal device for storage therein, the data package including at least one cryptographic key specific to said personal device **[Mauro: par. [0038]; par. [0034], lines 1-7; A secure unit 240 to perform all secure processing and store all "sensitive" data (e.g. cryptographic key) by various cryptographic technique]**;

(e) wherein the at least one personal device includes a processor configured for encrypting the received data package with the unique secret chip key and transferring a resulting backup data package back to the secure processing point **[Mauro: par. [0036], lines 8-11; "secure processor 250 retrieves data stored within memory 254, processor and/or encrypts the retrieved data, and may send the data to external elements (e.g., main processor 230 via bus 262)]**; and

(m) storing the certificate in the device **[Mauro: par. [0010]; storing certificate in secure storage of data]**;

(n1) storing the unique device identity and the certificate **[Mauro: par. [0010]; storing certificate in secure storage of data; par. [0055]; the certificate is issued and signed by a trusted certificate authority that certifies the remote terminal's identity; par. [0063]; certificate containing identity verification information for the remote terminal].**

Mauro does not explicitly disclose,

(f) wherein the processor of the secure processing point is arranged for storing the received backup data package in association with the unique chip identifier in a permanent public database separated from the personal device;

(g) wherein the processor of the secure processing point further is arranged for:

(h) associating a unique device identity with the unique chip identifier;

(l) signing the result of the association with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the personal device, thereby generating a certificate for the unique device identity;

(n) storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database.

However, Craft discloses the processor of the secure processing point is arranged for storing the received backup data package in association with the unique chip identifier in a permanent public database separated from the personal device **[Craft: par. [0043], lines 1-6 and figure 2. A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database].**

Craft further discloses wherein the processor of the secure processing point further is arranged for:

(h1) associating a unique device identity with the unique chip identifier **[Craft: par. [0015]; par. [0041]; a unique device identity is associated with client device; CPU chip is equivalent to unique chip identifier]**;

(l) signing the result of the association with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the personal device, thereby generating a certificate for the unique device identity **[Craft: par. [0036]; "a data can be signed by computing a digital signature from the data and the private key of signer"; a data signed by computing a digital signature using private key, thereby generating a certificate]**;

(n) storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database **[Craft: par. [0043], lines 1-6 and figure 2; A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database]**;

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the system of Mauro by including the processor of the secure processing point is arranged for storing the received backup data package of Craft because it would ensure security of the communication between client devices and servers **[par. [0013], lines 1-4, Craft et al.]**.

Mauro and Craft are not so clear of disclosing a unique device identity and associating a unique device identity with the unique chip identifier;

However, Chien discloses methods and apparatus for anonymous user identification and content personalization in wireless communication, wherein associating a unique device identity with the unique chip identifier **[Chien: Col. 3; lines 15-20; Col. 3, lines 55-60; Col. 4, lines 1-32; fig. 1; Wireless communication device includes a device serial number 102 and a SIM_ID 107; Col. 4, lines 28-32; An International Mobile Station Equipment Identity (IMEI) can be used as a device identifier; fig. 2; Col. 4, lines 40-50; retrieving personalization parameters such as a device serial number as a SIM_ID; Col. 6, lines 54-57].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the method of Mauro and Craft by including the teaching of Chien wherein associating a unique device identity with the unique chip identifier to provide anonymous content personalization in wireless communication network **[Chien: Col. 2, lines 34-42].**

Although the combination of Mauro, Craft, and Chien teach the claimed subject matter, they are not so clear of disclosing the secure processing point being separated from the personal device. On the hand, Okimoto teaches this limitation in Column 5 **[Okimoto: Col. 5, lines 52-53].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Mauro, Craft, and Chien by including teaching of Okimoto because it would securely deliver encrypted content on demand with access control **[Col. 3, lines 67 to Col. 4, line 1, Okimoto].**

As per Claim 11:

Claim 11 is essentially the same as claim 3 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 12:

Claim 12 is essentially the same as claim 4 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 14:

Claim 14 is essentially the same as claim 6 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 16:

Claim 16 is essentially the same as claim 8 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 17:

The combination of teaching Mauro, Craft, Chien, and Okimoto teach the claimed subject matter.

Mauro further discloses:

reading a unique chip identifier from a read-only storage of the personal device **[Mauro: par. [0038]); A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier) via a secure operation (e.g., during the manufacturing phase) and become available for use thereafter (e.g. retrieving a unique chip identifier)]**;

Craft further discloses:

transmitting the chip identifier to a public database **[Craft: par. [0043], lines 1-6 and figure 2; A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database].**

receiving from the public database a backup data package which has been assembled and stored in accordance with claim 1 and corresponding to the transmitted chip identifier **[Craft: par. [0015]; lines 8-15; "The client forms a request message, which includes the client serial number, encrypt the request with the server public key ad send the download request to the server… the client private key embedded in the client"];** and

storing the received backup data package in the personal device **[Craft: par. [0015]; lines 11-15; "The client serial number in the received request is used to search for client public key that corresponds to the client private key embedded in the client"].**

As per Claim 25:

Claim 25 is essentially the same as claim 1 except that it sets forth the claimed invention as an apparatus further comprising a processor **[Mauro, fig. 3; box 250, box 230]** rather a method and rejected under the same reasons as applied above.

As per Claim 27:

Claim 27 is essentially the same as claim 1 except that it sets forth the claimed invention as a device rather a method and rejected under the same reasons as applied above.

Claims 18, 20-21, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mauro** (US 2002/0147920) in view of **Craft** et al. (US 2002/0150243) further in view of **Okimoto** et al. (US 6,978,022 B2).

As per claim 18:

Mauro discloses a personal device comprising:

(a) an integrated circuit chip with a unique chip identifier in a read-only storage and a unique secret chip key in a tamper-resistant secret storage **[Mauro: par. [0038], lines 1-4. A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier); par. [0039], lines 9-11; "secure processor 250 and memory 254 are implemented as two separate units enclosed within a secure and/or tamper resistance/evident unit];**

(c) a memory for storing a received data package including at least one cryptographic key **[Mauro: par. [0037], lines 1-3. A flash memory is a form of non-volatile memory which is equivalent to memory (130); par. [0034], lines 1-7. A secure unit 240 to perform all secure processing and store all "sensitive" data (e.g. cryptographic key) by various cryptographic technique].**

(f) a read-only memory storing a manufacturer public signature key, wherein the memory for storing the received data package is further for storing a received certificate, which

corresponds to a certificate stored in association with the backup data package in the public database and which has been signed with a manufacturer private signature key corresponding to the manufacturer public signature key **[Mauro: par. [0077]; "The signature generation can be performed based on any one of the digital signature and encryption algorithms. Secure processor 250 may further provide the certificate that includes the remote terminal's public key"].**

Mauro does not explicitly disclose:

(b) "a processor configured for outputting the unique chip identifier";

(d) "where the processor is further configured for encrypting the received data package with the unique secret chip key and outputting a resulting backup data package to a permanent public database separated from said personal device".

However, Craft discloses:

(b) a processor configured for outputting the unique chip identifier **[Craft: par. [0041], lines 7-9; "each CPU chip is assigned a unique client serial number].**

(d) wherein the processor is further configured for encrypting the received data package with the unique secret chip key and outputting a resulting backup data package to a permanent public database separated from said personal device **[Craft: abstract , par. [0043], lines 1-6 and figure 2. Encrypting a request which includes a client serial number (216) is equivalent to encrypt the received data package with the unique secret chip key. The client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the system of Mauro by including the processor of the secure processing point is arranged for storing the received backup data package of Craft because it would ensure security of the communication between client devices and servers **[par. [0013], lines 1-4, Craft et al.].**

Although the combination of Mauro and Craft teaches the claimed subject matter, they are not so clear of disclosing the secure processing point being separated from the personal device. On the hand, Okimoto teaches this limitation in Column 5 **[Okimoto: Col. 5, lines 52-53].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the device of Mauro and Craft by including the teaching of Okimoto because it would securely deliver encrypted content on demand with access control **[Col. 3, lines 67 to Col. 4, line 1, Okimoto].**

As per claim 20:

The combination of Mauro, Craft, and Okimoto teach the subject matter as described above. Craft further teaches the personal device as claimed in claim 18, wherein the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device **[Craft: par. [0038], figure 2; "a data processing system for secure communication of application code and content using permanent, hardware-embedded, cryptographic key"].**

As per claim 21:

Craft further teaches the personal device as claimed in claim 20, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key **[Craft: par. [0038], lines 1-5; par. [0060], lines 20-24. The symmetric key is a cryptographic key which uses trivially cryptographic key for both decryption and encryption].**

As per claim 23:

Craft further teaches the personal device as claimed in claim 20, wherein the at least one key to be used for a secure, key based communication channel includes a private/public key pair **[Craft: par. [0038], par. [0032], "Public key cryptography requires each party involved in a communication or transaction to have a pair of key, called the public key and the private key"]**

Claims 7 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable **Mauro** (US 2002/0147920) in view of **Craft et al**. (US 2002/0150243), further in view of **Chien** (US 7,551,913 B1), further in view of **Okimoto** et al. (US 6,978,022 B2), and further in view of **Ginter** et al. (US patent 5,892,900).

As per Claim 7:

The combination of teaching Mauro, Craft, Chien, and Okimoto teach the claimed subject matter.

Craft further discloses generated by the secure processing point during assembly of the device **[Craft: par. [0042], lines 1-6. Each client CPU chip has a cryptographic unit (public/private key) that has been manufactured to contain programmable memory storage].**

Mauro, Craft, Chien, and Okimoto do not explicitly disclose, "the private/public key pair is generated and store in advance in a secure database before assembly of the device, in which latter case the cryptographic keys stored in advance of assembly are removed from the secret database after reception of the backup data package".

However, Ginter discloses how to generate and store in advance in a secure database before assembly of the device, in which latter case the cryptographic keys stored in advance of assembly are removed from the secret database after reception of the backup data package **[Ginter: Col. 169, lines 9-17; claim 101. An electronic appliance 600 updates its secure database 610 and/or SPU 500. If an information is received, an end user's electronic appliance 600 requesting the electronic appliance to delete the information that has been transferred. The information comprises at least one or more cryptographic keys**].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the teaching of Mauro, Craft, Chien, and Okimoto by including how to store the cryptographic keys in advance and removed from the secret database as suggested by Ginter because it would allow the secure database 610 item is updated or modified, a new encryption key can be generated for updated item **[Ginter, Col. 171, lines 43-46].**

As per Claim 15:

Claim 15 is essentially the same as claim 7 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

Claims 5 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mauro** (US 2002/0147920) in view of **Craft** et al. (US 2002/0150243) further view of **Chien** (US 7,551,913 B1), further in view of **Okimoto** et al. (US 6,978,022 B2), and further in view of **Audebert** et al. (US 2003/0086571 A1).

As per Claim 5:

The combination of teaching Mauro, Craft, Chien, and Okimoto teach the claimed subject matter.

Mauro, Craft, Chien, and Okimoto do not explicitly disclose wherein the symmetric key is generated as a function of a master key and the unique device identity.

However, Audebert teaches a system and method for generating symmetric keys within a personal security device having minimal trust relationships, wherein the symmetric key is generated as a function of a master key and the unique device identity **[Audebert: fig. 2B; par. [0041]; master key 280, PSD's serial number 65A, and composite key 210].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the teachings of Mauro, Craft, Chien, and Okimoto by including the teaching as suggested by Audebert to provide a method and system for generating a composite symmetric key, which securely incorporates information from each service provider

contained in a Personal security devices (PSD) and is only known to a trusted third party **[Audebert: par. [0011]].**

As per Claim 13:

Claim 13 is essentially the same as claim 5 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

Claims 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mauro** (US 2002/0147920) in view of **Craft** et al. (US 2002/0150243) further in view of **Okimoto** et al. (US 6,978,022 B2), and further in view of **Audebert** et al. (US 2003/0086571 A1).

As per claim 22:

The combination of Mauro, Craft, and Okimoto teach the subject matter as described above. Mauro, Craft, and Okimoto do not explicitly disclose wherein the symmetric key is generated as a function of master key and the unique device key.

However, Audebert teaches a system and method for generating symmetric keys within a personal security device having minimal trust relationships, wherein the symmetric key is generated as a function of a master key and the unique device identity **[Audebert: fig. 2B; par. [0041]; master key 280, PSD's serial number 65A, and composite key 210].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the teachings of Mauro, Craft, and Okimoto by including the teaching as suggested by Audebert to provide a method and system for generating a composite

symmetric key, which securely incorporates information from each service provider contained in a Personal security devices (PSD) and is only known to a trusted third party **[Audebert: par. [0011]].**

Claims 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mauro** (US 2002/0147920) in view of **Craft** et al. (US 2002/0150243) further in view of **Okimoto** et al. (US 6,978,022 B2), and further in view of **Chien** (US 7,551,913 B1).

As per claim 24:

Craft further teaches the personal device as claimed in claim 18, wherein the personal device is a wireless communications terminal **[Craft: par. [0025], lines 13-16. Personal digital assistant (PDAs, client 107) is equivalent to a wireless personal device]** but does not explicitly disclose a wireless communication terminal which has an unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network.

However, Chien discloses a methods and apparatus for anonymous user identification and content personalization in wireless communication, wherein an unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network **[Chien: Col. 3; lines 15-20; Col. 3, lines 55-60; Col. 4, lines 1-32; fig. 1; Wireless communication device includes a device serial number 102 and a SIM_ID 107; Col. 4, lines 28-32; An International Mobile Station Equipment Identity (IMEI) can be used as a device identifier; fig. 2; Col. 4, lines 40-50; retrieving personalization parameters such as a device serial number as a SIM_ID; Col. 6, lines 54-57].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the method of Mauro and Craft by including the teaching of Chien wherein an unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network to provide anonymous content personalization in wireless communication network **[Chien: Col. 2, lines 34-42].**

Conclusion

The examiner requests, in response to this Office action, support be shown for language added to any original claims on amendment and any new claims. That is, indicate support for newly added claim language by specifically pointing to page(s) and line number(s) in the specification and/or drawing figure(s). This will assist the examiner in prosecuting the application. Failure to show support can result in a non-compliant response.

When responding to this office action, Applicant is advised that if Applicant traverses an obviousness rejection under 35 U.S.C. 103, a reasoned statement must be included explaining why the Applicant believes the Office has erred substantively as to the factual findings or the conclusion of obviousness See 37 CFR 1.111(b).

Additionally Applicant is further advised to clearly point out the patentable novelty which he or she thinks the claims present, in view of the state of the art disclosed by the references cited or the objections made. He or she must also show how the amendments avoid such references or objections See 37 CFR 1.111(c).

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

US 7187919 B2 to Fukuzato; Atsushi;

US 5983117 A to Sandler; Howard Martin et al.;

US 5887253 A to O'Neil; Douglas Rutherford et al.;

US 20020013898 A1 to Sudia, Frank W. et al.;

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Orgad Edan can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

November 6, 2009

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434